サイバーセキュリティ

Topical Requirement

トピック別要求事項

ユーザーガイド

The Institute of
Internal Auditors

目次

トピック別要求事項の概要

トピック別要求事項は、「グローバル内部監査基準™（Global Internal Audit Standards™）」及び「グローバル・ガイダンス」と共に、「専門職的実施の国際フレームワーク（International Professional Practices Framework®）」の不可欠な構成要素である。内部監査人協会は、トピック別要求事項を「グローバル内部監査基準」と共に使用されなければならず、これらは、必須事項に関する権威ある基礎を提供する。より詳細な情報は、本ガイド内の基準の記述を参照のこと。

トピック別要求事項は、内部監査人が広く知られたリスク領域を扱う際に、高い監査品質と一貫性を促進することを目的として公式化したものである。トピック別要求事項は、各トピックの要求事項の対象に関連する個々のアシュアランス業務を実施するための基礎を確立し、関連する評価規準を提供する（基準 13.4「評価規準」）。トピック別要求事項への適合は、個々のアシュアランス業務では必須であり、アドバイザリー業務では評価が推奨される。トピック別要求事項は、個々のアシュアランス業務を実施する際に考慮すべきすべての潜在的な側面をカバーすることを意図しているのではなく、むしろ、トピックに関する一貫性のある信頼性の高い評価を可能にするための最低限の要求事項を提供することを意図している。

トピック別要求事項は、IIA の「３ラインモデル」及び「グローバル内部監査基準」と密接に関連している。ガバナンス、リスク・マネジメント及びコントロール・プロセスは、基準 9.1「ガバナンス、リスク・マネジメント及びコントロールの各プロセスの理解」と整合するトピック別要求事項の主要な構成要素である。「３ラインモデル」を参照すると、ガバナンスは取締役会／統治機関に、リスク・マネジメントは第２ラインに、コントロール又はコントロール・プロセスは第１ラインに関連している。経営管理者は第１ラインと第２ラインの両方に含まれるが、内部監査機能は、独立にして客観的なアシュアランス提供者として第３ラインに位置付けられ、取締役会／統治機関に報告する（原則 8「取締役会による監督」）。

適用可能性、リスク及び専門職としての判断

内部監査部門が、トピック別要求事項が存在する対象に関する個々のアシュアランス業務を実施する場合、又は他のアシュアランス業務の中にトピック別要求事項の側面が特定される場合には、トピック別要求事項に従わなければならない。

基準に記載されているように、リスク評価は、内部監査部門長の監査計画を策定する際の重要な要素である。内部監査の計画に含まれる個々のアシュアランス業務を決定するには、少なくとも年１回、組織体の戦略、目的及びリスクを評価する必要がある（基準 9.4「内部監査の計画」）。個々のアシュアランス業務を計画する際、内部監査人は、その業務に関連するリスクを評価しなければならない（基準 13.2「個々の内部監査業務におけるリスク評価」）。

リスクベースの内部監査の計画策定プロセスにおいて、各トピックの要求事項の対象が特定され、監査計画に含まれている場合には、該当する業務において、各トピックの要求事項に概説されている要求事項を用いて評価しなければならない。また、内部監査人が業務を実

施し（監査計画に含まれているかいないかにかかわらず）、各トピックの要求事項の要素が特定された場合、各トピックの要求事項は、業務の一環として適用可能性を評価しなければならない。最後に、当初は計画に含まれていなかったが、そのトピックを含む業務を依頼された場合、トピック別要求事項の適用可能性を評価しなければならない。

専門職としての判断は、トピック別要求事項の適用において重要な役割を果たしている。リスク評価は、内部監査の計画にどのような業務を含めるかについて、内部監査部門長の決定を後押しする（基準 9.4「内部監査の計画」）。さらに、内部監査人は、専門職としての判断を用いて、各業務でどのような側面をカバーするかを決定する（基準 13.3「個々の内部監査業務の目標及び範囲」、基準 13.4「評価規準」、基準 13.6「監査プログラム」）。付録 A「実務上の適用事例」では、内部監査人が、どのようにして、トピック別要求事項が適用されるかどうかを判断するかについて説明している。

トピック別要求事項の各トピックの要求事項は適用可能性について評価されたという証拠を、要求事項の除外を説明する根拠を含めて、保持しなければならない。トピック別要求事項への適合は、基準 14.6「個々の内部監査業務の文書化」に記載されているように、監査人の専門職としての判断を用いて文書化されなければならない。

サイバーセキュリティのトピック別要求事項は、考慮すべきコントロール・プロセスの最低基準を設定しているが、サイバーリスクを非常に高いと評価する組織体は、さらに追加的な側面を評価しなければならない場合もある。

内部監査部門長は、内部監査部門がトピック別要求事項に関する個々の内部監査業務を実施するために必要な知識を有していないと判断した場合には、当該業務をアウトソーシングする場合もある（基準 3.1「専門的能力」、基準 7.2「内部監査部門長の適格性」、基準 10.2「人的資源の管理」）。その場合でも、アウトソーシングによって、内部監査部門が、トピック別要求事項に適合する責任を免れるわけではない。内部監査部門長は、適合性を確保するための最終的な責任を保持する。さらに、内部監査部門長が内部監査の資源が不足していると判断した場合、内部監査部門長は、監査資源の不足の影響及び対応方法について、取締役会に報告しなければならない（基準 8.2「監査資源」）。

パフォーマンス、ドキュメンテーション及びレポーティング

また、内部監査人は、トピック別要求事項を適用する場合、基準に準拠し、「ドメイン Ⅴ：内部監査業務の実施」に従って業務を実施しなければならない。ドメイン Ⅴ の基準では、監査計画の立案（13 原則「個々の内部監査業務の計画の効果的な策定」）、監査業務の実施（14 原則「個々の内部監査業務の実施」）、監査結果の伝達（15 原則「個々の内部監査業務の結論のコミュニケーション及び改善措置の計画のモニタリング」）について規定している。

トピック別要求事項は、監査人の専門職としての判断に基づき、内部監査の計画又は個々の内部監査業務の監査調書に文書化することができる。 1 つ又は複数の個々の内部監査業務が、要求事項をカバーしている場合がある。また、すべての要求事項が該当するとは限らない。適用除外を説明する論理的根拠を含め、トピック別要求事項は適用可能性について評価され

たという証拠を保持しなければならない。

付録 C の任意の文書作成ツールは、内部監査人が実施する業務（work）を文書化するための参考資料として使用することができる。

品質のアシュアランス

基準は、内部監査部門長に対し、内部監査部門のあらゆる側面をカバーする品質のアシュアランスと改善のプログラムを策定、実施、維持することを求めている（基準 8.3「品質」）。その結果は、取締役会及び最高経営者に報告されなければならない。伝達事項には、内部監査機能の基準への適合状況とパフォーマンス目標の達成状況について含めなければならない。

トピック別要求事項への適合性は、品質評価において評価される。品質評価の準備として、内部監査人は付録 C として提供されたツールを使用することができる。

サイバーセキュリティ

サイバーセキュリティは、あらゆる組織体のほとんどの技術的側面に関連する広範なテーマである。情報技術に加え、サイバーセキュリティは一般的にビジネス・プロセスの一部であるため、内部監査人は、個々のアシュアランス業務を計画し、対象範囲を決定し、個々の内部監査業務を実施する際には、サイバー関連のリスクを評価する必要がある。

米国商務省の傘下の国立標準技術研究所（NIST）は、サイバーセキュリティを単に「サイバー攻撃からサイバー空間の使用を保護又は防御する能力」と定義している。サイバーセキュリティの要求事項は、不正ユーザーや悪意のあるサイバー脅威からのリスクを軽減するために組織体が保護する外部境界線に焦点を当てている。サイバーセキュリティは、包括的な情報セキュリティの一部であり、NIST は「機密性、完全性及び可用性を提供するために、不正アクセス、使用、開示、中断、改変あるいは改ざん、又は破壊から情報と情報システムを保護すること」と定義している。

サイバーセキュリティのトピック別要求事項には以下が含まれる。

- ガバナンス - 組織体の目標、方針及び手続を支援する基礎となるサイバーセキュリティへの対応目標と戦略を明確に定義する。
- リスク・マネジメント - サイバーリスクを迅速に上申するプロセスを含む、サイバー脅威を識別、分析、管理、モニタリングするプロセス
- コントロール - サイバーリスクを軽減するために経営管理者が確立し、定期的に評価するコントロール・プロセス

考慮すべき事項

内部監査人は、サイバーセキュリティのトピック別要求事項の評価を支援するために、以下の考慮すべき事項を使用することができる。これらの考慮すべき事項は、要求事項を相互参照するものであり、例示であるが強制ではない。内部監査人は、評価に何を含めるかを決定する際に、専門職としての判断に基づくべきである。

ガバナンスに関し、考慮すべき事項

ガバナンス・プロセスが、サイバーセキュリティのリスクへの対応目標にどのように適用されているかを評価するために、内部監査人は以下の点をレビューすることがある。

A. 取締役会が、最高情報セキュリティ責任者（CISO）など情報セキュリティ機能の責任者から提供されたサイバーセキュリティの最新情報を定期的（通常は四半期ごと）にレビューしているという証拠を含め、サイバーセキュリティの戦略計画と目標が正式に文書化されている。証拠には、以下に関する報告が含まれる。
   - 戦略目標の達成をモニタリングする。
   - サイバーセキュリティのリスクへの対応目標と目的をサポートするための予算ニーズ
   - リスクと内部統制（是正の進捗状況を含む）に焦点を当てる。
   - 成功を測定するための主要業績評価指標（KPI）
   - サイバーセキュリティのリスクへの対応が可能な人材を、雇用、教育訓練、育成する必要性

B. サイバーセキュリティ・プロセスの管理に使用される方針、手続、及びその他の関連文書には以下が含まれる。
   - 少なくとも年 1 回の見直しと更新を行う方針。新たなサイバーリスクの発生により、見直しや更新をより頻繁に行う必要が生じる場合もある。
   - 方針と手続がサイバーセキュリティのリスクへの対応業務を支援するのに十分かどうかを判断するプロセス
   - サイバーセキュリティ・プロセスと内部統制を強化するために広く採用されているフレームワーク（NIST、COBIT など）

C. サイバーセキュリティのリスクへの対応目標の達成を支援する役割と責任。これには、サイバーセキュリティ機能が、組織体の支援を得るために十分な可視性を有する組織体内のレベルに報告されるようにする仕組みも含まれる。
   - サイバーセキュリティの役割を担う人材の知識、スキル及び能力を定期的に評価するプロセス

D. 関連するステークホルダー（例えば、最高経営者、業務、リスク・マネジメント、人事、法務、コンプライアンス、戦略的ベンダーなど）との個々の内部監査業務の証拠（既存及び新たに発生するサイバーリスクや既知の潜在的脆弱性に関するコミュニケーションを含む）。コミュニケーションの証拠には、会議の議事録、報告書、電子メールなどが含まれる。

リスク・マネジメントに関し、考慮すべき事項

リスク・マネジメント・プロセスがサイバーセキュリティのリスクへの対応目標にどのように適用されているかを評価するために、内部監査人は以下の点をレビューすることがある。

A. 脅威や脆弱性がどのように存在するかを含め、組織体がサイバーセキュリティのリスクをどのように評価し、管理しているか。
   - 最初に識別され、報告される方法
   - 組織体の目標達成に対するリスクを評価するために分析される方法
   - リスクを許容可能なレベルまで低減するための行動計画を含む低減方法
   - 脅威が完全に解決されるまで継続的に報告する計画を含む、モニタリング方法

B. 組織体が、情報技術、全社的リスク・マネジメント、人事、法務、コンプライアンス、業務、経理、財務などの機能領域から、サイバーセキュリティリスク・マネジメントに関する定期的な情報をどのように入手しているか。情報入手のために、機能横断的なサイバーセキュリティチーム又は IT ステアリング・コミッティを活用することもある。

C. 組織体がサイバーセキュリティ・リスク・マネジメントの遂行責任と説明責任をどのように個人又はチームに割り当てているか。
   - 責任者は、継続的なサイバーセキュリティのリスクの最新情報を定期的（四半期ごと、月ごと、又は必要に応じて）に組織体全体に伝達する必要があり、リスク軽減戦略のためのリソース要件も含めることができる。

D. 脅威又はリスクのレベルがどのように評価され、割り当てられ、優先順位付けされるかを含む、サイバーセキュリティのリスクのエスカレーション・プロセス。レビューには、以下を特定することが含まれる。
   - 組織体が定義したリスクレベル（高、中、低など）と、各リスクレベルの詳細な説明、及び各リスクカテゴリーのエスカレーション手順
   - 現在識別されているサイバーセキュリティのリスクのリストと、各リスク事象の軽減状況
   - 適用される法律、規制、コンプライアンス要件
   - 財務リスクと非財務リスク（例えばレピュテーション）の両方が影響する。

E. サイバーセキュリティのリスクを経営管理者と従業員に伝えるプロセス
   - 組織体の意識をテストし、追跡するために、抜き打ちで模擬的なフィッシング・キャンペーンを行うなど、定期的（少なくとも年 1 回）に従業員のサイバーセキュリティ・トレーニングを行う。
   - 既存のサイバーセキュリティ問題の改善に関する最新情報
   - 取締役会及び最高経営者への更新を含む、コンプライアンス違反のモニタリング
   - 組織体のリスク選好度やリスク許容度が変化した場合に、脅威を再評価する。

F. 組織体がインシデント対応と復旧に関して実施しているプロセス
   - 組織体の業務が時とともに変化するにつれて見直され、更新される、文書化された計画。計画には以下が含まれる。
     - インシデントの検出と報告方法
     - 被害を拡大させないために、どのように事件を収束させるか。
     - 業務を再開するために、組織体がどのように復旧し、対応するか。
     - 事故をどのように分析し、教訓を明らかにし、将来の同様の出来事をどのように防ぐか。
   - 定期的（少なくとも年 1 回）にテスト（卓上演習）を行い、その結果を最高経営者及び関係ステークホルダーに報告する。テストからアクションプランが生まれることもある。

コントロール・プロセスに関し、考慮すべき事項

コントロール・プロセスがサイバーセキュリティのリスクへの対応目標にどのように適用されているかを評価するために、内部監査人は以下の点をレビューすることがある。

A. 効果的なサイバーセキュリティ内部統制環境を構築するための経営管理者のアプローチには以下が含まれる。
   - 組織体のリスクアセスメント・プロセスに基づき、増大するリスクを軽減し、機密性、重要性、個人情報、又は機密データを保護するために必要な内部統制を評価し、実施する。
   - 主要なサイバーセキュリティ・コントロールを維持するためのリソース要件を決定する。
   - ベンダーに基づくコントロールを統制環境の一部として考慮すること。これには、取引関係を開始する前及び取引関係期間を通じて、ベンダーからの受託会社の内部統制に係る保証報告書（SOC：Service Organization Controls）をレビューすることが含まれる。
   - サイバーセキュリティ・コントロールがリスクを軽減し、サイバーセキュリティのリスクへの対応目標の達成を支援する方法で機能していることを定期的にテストする。
   - 内部統制の不備を改善するためのプロセス、又は内部監査機能もしくは他のアシュアランス提供者が実施した評価（例えば、侵入テスト）による発見事項に対処するためのプロセス

B. サイバーセキュリティの専門家を採用し育成するための組織体の人材管理プロセス。これには、サイバーセキュリティの専門家の能力を向上させ、技術的な知識をサポートし、新たな問題に対する組織体の認識を向上させる機会を、組織体がどのように特定しているかを含む。
   - 例えば、研修への参加、知識共有グループへの参加、サイバー関連資格の取得を含む継続的専門教育などである。

C. 日常業務に焦点を当てた、新たなサイバーセキュリティの脅威と脆弱性を継続的に識別、優先順位付け、モニタリング、報告するための経営管理者のプロセスレビューには、人工知能（AI）の活用など、新しい技術や出現しつつある技術に関連する脅威や脆弱性を評価するためのプロセスが確立されていることを含めることがある。

D. ハードウェア、ソフトウェア、ベンダー・サービスの導入、使用、メンテナンス及び廃棄を含むライフサイクル全体を通じて、IT 資産を管理・保護するために確立された経営管理者のプロセスとコントロール。ハードウェアには、サーバー、ネットワーク機器（ルーターやファイアウォールなど）、デスクトップ、ノートパソコン、携帯電話、タブレット端末、周辺機器などが含まれる。ソフトウェアには、オペレーティング・システム（Windows など）、ERP ソフトウェア、アプリケーション、ウイルス対策プログラムなどが含まれる。ハードウェアとソフトウェアの考慮事項には、以下のようなものがある。
   - 暗号化、ウイルス対策ソフトウェア、モバイル機器管理、複雑なパスワード要件、認証のための仮想プライベート・ネットワーク（VPN）／ゼロ・トラスト・ネットワーキング（ZTN）、ファームウェアの定期的な更新などの組織体の使用
   - 会社から支給されたハードウェアが、発行時に適切なセキュリティ構成を持つことを保証し、資産が廃棄される際には適切に処分する資産管理プロセス
   - データベース関連の管理には、ユーザー及び管理者のアクセス制限、暗号化の使用、データベースのバックアップとテスト、強力なネットワーク・セキュリティ管理の存在などが含まれる。
   - システム開発ライフサイクル（SDLC）において、サイバーセキュリティの脅威や脆弱性をどのように考慮するか。
   - 開発、セキュリティ、運用（DevSecOps）が採用するアプローチは、ソフトウェア開発プロセスにサイバーセキュリティのリスクへの対応を確実に組み込み、脆弱性を積極的に識別することを目的としている。

E. サイバーセキュリティを強化するために使用されるプロセスには以下が含まれる。
   - サイバーセキュリティのリスクを最小化するためのセキュリティ設定の構成
   - モバイル機器の管理（電子メールやアプリケーションの使用を含む）は、サイバーセキュリティのリスクを軽減し、ユーザーデバイスが侵害された場合にリモートで管理できるように構成されている。
   - ハードドライブに保存されている情報のような「静止状態」のデータや、電子メールの暗号化のような「転送中」のデータに対する暗号化の使用
   - サーバー又はソフトウェア（オペレーティング・システムなど）に、最新のセキュリティ・リリースのパッチを適用すること。
   - 多要素認証（MFA）や、定期的に有効期限が切れる複雑なパスワードを持つ固有のユーザー ID の使用などのユーザーアクセス管理
   - 可用性とリソースの利用が適切に行われているかどうかを判断するために実施されているモニタリング・コントロールにより、パフォーマンスを脅かすサイバーセキュリティ上の潜在的な問題のレビューと分析が可能になる。
   - ソフトウェアが本番稼動する前にサイバーセキュリティの脆弱性を識別し、対処するために、サイバーセキュリティを SDLC に統合する。

F. 組織体の境界を保護するネットワーク関連の管理（組織体の利用方法を含む）
   - ネットワークのセグメンテーション
   - ファイアウォール
   - ユーザーアクセス・コントロール
   - 外部接続と内部接続の両方に制限がある。
   - 相互接続されたネットワークのモノのインターネット（IoT）を取り巻くコントロール
   - サイバーセキュリティ攻撃を防止、検出、回復するための侵入検知／防止システム

G. 電子メール、インターネットブラウザ、ビデオ会議、メッセージング（Zoom、MS Teams、その他）、ソーシャルメディア、クラウド、ファイル共有プロトコルなどのサービスに適用される、エンドポイントコミュニケーションセキュリティを取り巻くコントロール。コントロールには、特定のファイル拡張子（.exe ファイルなど）の使用制限や、ファイル共有のための多要素認証などが含まれる。

付録 A. 実務上の適用事例

以下の例は、サイバーセキュリティのトピック別要求事項が適用されるシナリオを説明するものである。

例 1： 内部監査の計画に含まれる内部監査業務において、サイバーセキュリティのリスクが識別されている

内部監査部門がリスクベースの計画プロセスを完了し、内部監査の計画にサイバーセキュリティに関する 1 つ又は複数の業務を含める場合、当該業務を実施する際に、このトピック別要求事項が必須となる。適合性は、内部監査の計画の 1 つ以上の業務に要求事項を含めることで達成できる。

サイバーセキュリティは広範なトピックであり、トピック別要求事項のすべての要求事項がすべての契約に適用されるとは限らない。内部監査人が専門的な判断を適用し、サイバーセキュリティに関するトピック別要求事項の 1 つ以上の要求事項が適用されず、結果として個々の内部監査業務から除外されるべきであると判断した場合、内部監査人は、それらの要求事項を除外する根拠を文書化し、保持しなければならない。例えば、いくつかの要求事項を除外する根拠として、内部監査部門が様々なサイバーセキュリティに関する業務をローテーションで実施していることや、当該業務におけるリスクの重要性が低いと判断したことなどが考えられる。

例 2： サイバーセキュリティに焦点を当てていない個々の内部監査業務において、サイバーセキュリティのリスクが識別された

内部監査人は、サイバーセキュリティに直接関係のないプロセスを評価しているときに、サイバーセキュリティのリスクを識別することがある。例えば、内部監査人は、サイバーセキュリティに焦点を当てていない業務で買掛金支払プロセスを評価することがあり、業務を計画する際にサイバーセキュリティのリスクを対象範囲として識別しないことがある。しかし、最初のウォークスルーを実施した後、内部監査人は、そのようなリスクは対象範囲であるべきであると判断する。例えば、内部監査人は、最初の発注依頼書のウェブベースの提出に関連するサイバーセキュリティのリスクを識別する（基準 13.2「個々の内部監査業務におけるリスク評価」）。

関連するリスクが識別されたら、内部監査人はサイバーセキュリティに関する主要な要求事項を確認し、どの要求事項が適用可能かを判断しなければならない。この例では、サイバーセキュリティ・ガバナンス・プロセス又はサイバーセキュリティ・リスク・マネジメント・プロセスを除外するかもしれない。内部監査人は、「サイバーセキュリティに関する主要な要求事項」の他の要求事項を除外する根拠を監査報告書に文書化し、その文書を保管しなければならない。

例 3： 当初、内部監査の計画に含まれていなかったサイバーセキュリティに関する業務の要請を受けた

取締役会、最高経営者、又は規制当局などのステークホルダーは、本来の監査計画以外のサイバーセキュリティ評価の実施を内部監査人に要請することがある。例えば、組織体がサイバー攻撃の標的になった場合、取締役会はサイバーセキュリティ・コントロールを評価するために内部監査業務を要請することがある。トピック別要求事項が適用され、要求事項を評価し、除外事項があれば文書化しなければならない。

付録 B. フレームワークへのマッピング

組織体は、COBIT や NIST などによるリスク・マネジメントやガバナンスのフレームワークを使用して、独自のサイバーセキュリティの取り組みを行っている可能性がある。内部監査人は、これらの関連フレームワークに基づいて、すでに監査プログラムとテスト手続を策定している可能性がある。内部監査人は、意図しているサイバーセキュリティ・コントロールのテストとトピック別要求事項とを照合し、十分なカバレッジを確保する必要がある。以下の表は、サイバーセキュリティの主要な要求事項を、一般的に使用されている 3 つのフレームワークに対応付けたものである。NIST サイバーセキュリティフレームワーク 2.0、COBIT 2019、NIST 800-53 である。これらの関連フレームワークは無償で容易に入手できることから、マッピングをした。

ガバナンス要求事項	関連フレームワーク		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. 正式なサイバーセキュリティ戦略と目標が設定され、定期的に更新されている。サイバーセキュリティ戦略をサポートするための資源や予算の検討も含め、サイバーセキュリティ目標の達成に関する最新情報が定期的に伝達され、取締役会によってレビューされている。	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. サイバーセキュリティに関する方針と手続は、統制環境を強化するために策定され、定期的に更新されている。	GV.PO-01; V.PO-02; GV.OV-01; GV.OV-02; V.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. サイバーセキュリティの目標をサポートする役割と責任が確立され、その役割を果たす個人の知識、スキル及び能力を定期的に評価するプロセスが存在する。	GV.RR-02; V.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07
D. サイバーセキュリティ環境における既存の脆弱性や新たな脅威について議論し、対処するために、ステークホルダーが関与している。ステークホルダーには、最高経営者、業務部門、リスク・マネジメント部門、人事部門、法務部門、コンプライアンス部門、ベンダーなどが含まれる。	GV.OC-02; V.RM-01; GV.RM-05; GV.RM-07; V.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02

リスク・マネジメント 要求事項	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. 組織体のリスク評価とリスク・マネジメントのプロセスには、サイバーセキュリティ上の脅威と、それが戦略目標の達成に及ぼす影響の識別、分析、低減及びモニタリングが含まれる。	GV.RM-01; V.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. サイバーセキュリティのリスク・マネジメントは組織体全体で実施する。情報技術、全社的リスク・マネジメント、人事、法務、コンプライアンス、業務、サプライチェーン、経理及び財務などの分野を含めてもよい。	GV.RM-01; V.RM-05; GV.RR-01; GV.RR-02; V.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. サイバーセキュリティのリスク・マネジメントに関する遂行責任と説明責任の所在が明確に定められ、また、リスクを低減し、新たなサイバーセキュリティの脅威を識別するために必要な資源を含め、サイバーセキュリティのリスクがどのように管理されているかを定期的にモニタリングし、報告する個人又はチームが特定されている。	GV.RR-01; V.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12
D. 組織体において策定されたリスク・マネジメント・ガイドラインまたは適用される法規制の要求事項に従って、許容できないレベルに達したサイバーセキュリティのリスク（顕在化したリスクまたは過去に識別され たリスク）を迅速に上申するプロセスを確立している。サイバーセキュリティのリスクの財務的影響と非財務的影響の両方を考慮する。	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. 経営管理者と従業員にサイバーセキュリティのリスクの認識を伝え、定期的に経営管理者が、問題、ギャップ、不備及びコントロールの機能不全を確認し、適時に報告し、是正するためのプロセスが確立されている。	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. 組織体は、サイバーセキュリティ・インシデントの検知、抑制、復旧、及び事後分析を含む、インシデント対応・復旧プロセスを導入している。インシデント対応・復旧プロセスは定期的にテストされている。	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

コントロール・プロセス 要求事項	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. 組織体のシステムとデータの機密性、完全性、可用性を保護するために、内部統制とベンダーに基づくコントロールの両方を確実に実施するためのプロセスが確立されていること。組織体のサイバーセキュリティのリスクへの対応目標の達成と問題の迅速な解決を促進する方法でコントロールが機能しているかどうかを判断するために、定期的に評価が実施されている。	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. サイバーセキュリティのリスクを低減するコントロールに関連する技術的能力を開発・維持するための教育訓練を含む、人材管理プロセスが確立されている。	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. 新たなサイバーセキュリティの脅威と脆弱性を継続的にモニタリング・報告し、サイバーセキュリティのリスクを低減するコントロールを改善する機会を識別、優先順位付け、実施するプロセスが確立されている。	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. サイバーセキュリティは、ハードウェア、ソフトウェア、ベンダー・サービスを含むすべての IT 資産のライフサイクル管理（導入、使用、メンテナンス及び廃棄）に含まれている。	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06
E. 構成、エンドユーザーデバイスの管理、暗号化、パッチ適用、ユーザーアクセス管理、可用性とパフォーマンスのモニタリングなど、サイバーセキュリティを強化するためのプロセスが確立されている。ソフトウェア開発（DevSecOps）にサイバーセキュリティへの考慮が含まれている。	PR.PS-01; R.PS-06; PR.DS-01; PR.DS-02; R.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. ネットワーク・アクセス・コントロールとセグメンテーション、ファイアウォールの使用と設置、外部ネットワークとの接続制限、仮想プライベートネットワーク（VPN）／ゼロトラストネットワークアクセス（ZTNA）、モノのインターネット（IoT）ネットワーク制御、及び侵入検知／防止システム（IDS と IPS）など、ネットワーク関連のコントロールが確立されている。	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. 電子メール、インターネットブラウザ、ビデオ会議、メッセージング、ソーシャルメディア、クラウド、及びファイル共有プロトコルなどのサービスに対して、エンドポイント・コミュニケーションのセキュリティ・コントロールが確立されている。	PR.DS-01; R.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

付録 C. 任意の文書作成ツール

内部監査人は、リスク評価に基づいて、専門職としての判断で要求事項の適用可能性を判断し、特定の要求事項の除外を適切に文書化することが期待されている。トピック別要求事項は、監査人の専門職としての判断に基づき、内部監査の計画又は個々の内部監査業務の監査調書に文書化することができる。１つ又は複数の個々の内部監査業務が、要求事項をカバーしている場合がある。また、すべての要求事項が該当するとは限らない。以下の印刷可能な書式は、サイバーセキュリティの主要な要求事項への適合を文書化するための一つの選択肢を提供するものだが、この使用は必須ではない。

サイバーセキュリティ - ガバナンス

要求事項	実施した範囲又は除外の理由	参照資料
A. 正式なサイバーセキュリティ戦略と目標が設定され、定期的に更新されている。サイバーセキュリティ戦略をサポートするための資源や予算の検討も含め、サイバーセキュリティ目標の達成に関する最新情報が定期的に伝達され、取締役会によってレビューされている。		
B. サイバーセキュリティに関する方針と手続は、統制環境を強化するために策定され、定期的に更新されている。		
C. サイバーセキュリティの目標をサポートする役割と責任が確立され、その役割を果たす個人の知識、スキル及び能力を定期的に評価するプロセスが存在する。		
D. サイバーセキュリティ環境における既存の脆弱性や新たな脅威について議論し、対処するために、ステークホルダーが関与している。ステークホルダーには、最高経営者、業務部門、リスク・マネジメント部門、人事部門、法務部門、コンプライアンス部門、ベンダーなどが含まれる。		

サイバーセキュリティ - リスク・マネジメント

要求事項	実施した範囲又は除外の理由	参照資料
A. 組織体のリスク評価とリスク・マネジメントのプロセスには、サイバーセキュリティ上の脅威と、それが戦略目標の達成に及ぼす影響の識別、分析、低減及びモニタリングが含まれる。		
B. サイバーセキュリティのリスク・マネジメントは組織体全体で実施する。情報技術、全社的リスク・マネジメント、人事、法務、コンプライアンス、業務、サプライチェーン、経理及び財務などの分野を含めてもよい。		
C. サイバーセキュリティのリスク・マネジメントに関する遂行責任と説明責任の所在が明確に定められている。リスクを低減し、新たなサイバーセキュリティの脅威を識別するために必要な資源を含め、サイバーセキュリティのリスクがどのように管理されているかを定期的にモニタリングし、報告する個人又はチームが特定されている。		
D. 組織体において策定されたリスク・マネジメント・ガイドラインまたは適用される法規制の要求事項に従って、許容できないレベルに達したサイバーセキュリティのリスク（顕在化したリスクまたは過去に識別され たリスク）を迅速に上申するプロセスを確立している。サイバーセキュリティのリスクの財務的及び非財務的な影響を考慮すべきである。		
E. 経営管理者と従業員にサイバーセキュリティのリスクの認識を伝え、定期的に経営管理者が、問題、ギャップ、不備及びコントロールの機能不全を確認し、適時に報告し、是正するためのプロセスが確立されている。		
F. 組織体は、サイバーセキュリティ・インシデントの検知、抑制、復旧、及び事後分析を含む、インシデント対応・復旧プロセスを導入している。インシデント対応・復旧プロセスは定期的にテストされている。		

サイバーセキュリティ - コントロール・プロセス

要求事項	実施した範囲又は除外の理由	参照資料
A. 組織体のシステムとデータの機密性、完全性、可用性を保護するために、内部統制とベンダーに基づくコントロールの両方を確実に実施するためのプロセスが確立されていること。組織体のサイバーセキュリティのリスクへの対応目標の達成と問題の迅速な解決を促進する方法でコントロールが機能しているかどうかを判断するために、定期的に評価が実施されている。		
B. サイバーセキュリティのリスクを低減するコントロールに関連する技術的能力を開発・維持するための教育訓練を含む、人材管理プロセスが確立されている。このプロセスは定期的に見直されている。		
C. 新たなサイバーセキュリティの脅威と脆弱性を継続的にモニタリング・報告し、サイバーセキュリティのリスクを低減するコントロールを改善する機会を識別、優先順位付け、実施するプロセスが確立されている。		
D. サイバーセキュリティは、ハードウェア、ソフトウェア、ベンダー・サービスを含むすべての IT 資産のライフサイクル管理（導入、使用、メンテナンス及び廃棄）に含まれている。		
E. 構成、エンドユーザーデバイスの管理、暗号化、パッチ適用、ユーザーアクセス管理、可用性とパフォーマンスのモニタリングなど、サイバーセキュリティを強化するためのプロセスが確立されている。ソフトウェア開発（DevSecOps）にサイバーセキュリティへの考慮が含まれている。		
F. ネットワーク・アクセス・コントロールとセグメンテーション、ファイアウォールの使用と設置、外部ネットワークとの接続制限、仮想プライベートネットワーク（VPN）／ゼロトラストネットワークアクセス（ZTNA）、モノのインターネット（IoT）ネットワーク制御、及び侵入検知／防止システム（IDS と IPS）など、ネットワーク関連のコントロールが確立されている。		
G. 電子メール、インターネットブラウザ、ビデオ会議、メッセージング、ソーシャルメディア、クラウド、及びファイル共有プロトコルなどのサービスに対して、エンドポイント・コミュニケーションのセキュリティ・コントロールが確立されている。		

内部監査人協会（The Institute of Internal Auditors（IIA））について

IIA は、全世界で 26 万人以上の会員を擁し、20 万人以上の公認内部監査人®（CIA®）資格を認定している国際的専門職団体である。1941 年に設立され、国際基準、認定資格、教育、研究、技術指導における内部監査専門職のリーダーとして世界中で認知されている。詳しくは、www.theiia.org を参照。

免責事項

IIA は、情報提供及び教育を目的として本文書を発行する。本文書は、個別具体的な状況に対する確答を提供することを目的とするものではなく、あくまでも指針として使用していただくものである。IIA は、特定の状況に直接関係する独立した専門家の助言を求めることを推奨する。IIA は、本稿のみに依拠する者に対して一切の責任を負わない。

著作権

2025 年 2 月

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1^407-937-1101